PRACTICAL PARANOID'S BOOK OF

COMPUTER SECURITY

By

Homer Otto Goodall, Jr

The Master of Ceremonies Stood up and announced, "I would like to introduce our guest speaker today. He was a war correspondent, self-taught computer security expert, controversial author, and controversial speaker." He sat down and a man that looked more like a mouse. He was a skinny, frail looking man with a boyish face. He took the podium. When he began to speak the public address system began to squeal. He turned it off and began to speak in a normal tone. His voice was booming, but almost mouse-like. He reminded me of the cartoon character Sniffles. He said, "Ladies, Gentlemen, Data thieves, Hackers, Spies, and other sorts I bid you welcome. The information that will be given in this talk will be what I learned from life not from a book, computer or any other source. As you know our freedoms are under attack. Plato said that Republics turn despotic over time. A despot is an auto-cratic tyranny, but I am not here to discuss politics, governments, and other ilk that was created by people." He then took a sip of water and coughed. He said, "excuse me. Dry throat and Post-nasal drip. First we will discuss the first layer of defense. Please look in your booklets. Please." He turned to page 1 in the booklet.

He continued, "The first line of defense should be a program that protects your system files from deletion. Some computer folks can get into your system and delete important system files. When this happens then wave bye-bye to your computer's operating system. It will crash. If you use one type of operating system then the hard drive will be reformatted and you will lose everything. Since we are talking about a freeware system we will keep on this subject. Some freeware programs have some of the features inactivated so a person will buy the entire program. We can use other programs to get the features not afforded by the freeware program. These programs or should I say program prevents this danger. See in the booklet that there is only two programs listed. I keep my System Protect on paranoid mode. It does not ask if I want a program to gain access to my computer it just denies it without any annoying messages. Anyone that doesn't keep their software and operating system updated then they are a fool. Remember I have a rather large hard drive and these are just guidelines."

FILE PROTECTION

System Protect-This is a very good program to prevent hackers from invading your system and deleting important files.

Winpatrol-This one works well with all the Antivirus programs.

A woman piped up and said, "Hey you are being paid by software companies for your opinion." The Practical Paranoid yelled, "Do you think I get paid by these people?! If you think that I will give you your money back and you can get out! If I was getting paid I sure as hell would not be in the financial shape I am in at the present time!" He calmed down and he relaxed as he continued his talk. He said, "Since we had gotten protecting you system from getting files destroyed and

thus crashing your computer. We will now move into the areas of spyware. Spyware is a program that can invade your online privacy. They can be anything from a Keylogger put on a system by your boss to tracking cookies. To the very extreme of spyware you have fake antivirus, fake spyware, and other programs. The companies will try to get money out of you with popup windows saying, "pay us $50.00 and we will remove the virus," but is there actually a virus? Of course not, but their antivirus is a virus. Their market plan is try to milk people for money. I did at one time use a two pronged attack for prevention of spyware. What is the best? Well, the one that I use had gotten very poor reviews, but it does the job. Yes, I still get tracking cookies on my system, but there are places I would not go on a network. Like places that are known hacker networks...ummm like keygen sites, hacking tool sites, and warez sites. Another little tidbit, don't use a peer-to-peer downloader because they are a serious security problem. I use a download manager that I download ebooks and such."

A boy waving his hand and got the practical paranoid's attention. The Practical Paranoid said, "yes son. Don't be shy. It is open forum." He said, "I have a peer-to-peer manager. Is there any way of securing it?" The Practical Paranoid said, "unfortunately son there is no way. Let me explain. Say in your house you leave through a door then you also enter through the same door. A peer-to-peer is like having two doors open in your house open. This software connects to an outside source and the information is brought inside your computer from this outside source. If you use one of these it is like leaving your doors to your home wide open when you leave. I use one that is on portable applications software. Most of my stuff isn't on my computer it is in this external drive. I do virus scans on this drive as often as I do them on my computer. Understand? You wouldn't leave your bicycle out in the front yard would you? Would you also leave a sign out in front of your house saying THE FRONT DOOR KEY IS UNDER A ROCK NEAR THE DOORMAT. THIEVES WELCOME? It sounds crazy, but this is why a person ought to be careful with these pieces of software." The boy shook his head and sat down.

"Now, that we had cleared that out of the way," replied the Practical Paranoid, "we can now go into keeping spyware off your system. Later on we will go into protecting children online and creating an insanely expensive suite of tools. Look in the book under antispyware. I generally use a two pronged attack against spy ware. Some that have an immunize feature then use them. Most of the ones listed in the booklet have an immunize feature."

ANTISPYWARE

It seems that the most logical is to keep spyware from being installed than to try to remove it in the first place. There are programs that have an inoculate feature on it. These are useful in keeping spyware off your system.

Spyware terminator-Integrated with Clam Antivirus plus the rest of the features it

works well as a secondary protection

Hijack this-Use the inoculate feature.

Spyware Blaster-Use the inoculate feature.

ArovaxShield-Be careful with this one.

Ad aware-This one is a piece of ad ware and it does work well. Be careful with it. It is ad supported software.

Spybot S&D-this one you must be extremely careful with it. This was the first one that I used and wound up crashing my media and word processor functions. It took me months to straighten out my system.

I have all these programs on my system and my system had been inoculated by the ones with this feature. I set the programs on paranoid mode for an extra level of protection. Being a practical paranoid I also use **System Protect** set on paranoid mode. System protect is my first defense. It keeps people from making changes on the system. You will get a lot of alerts every time someone is trying to make changes to your system, but eventually the program will “learn” which ones to allow and which ones to block. My security system is huge and experimental, but I will show you how to reduce the space used. Using an integrated system help to reduce the space used. One small problem with antispy programs is that the program will detect a part of your internet connect software and tell you it is a piece of spyware or adware. If you choose it to be deleted or removed then your internet connect software will crash. In a case like that then you will need to put the internet connect software back on your system. I’ve had some that told me that part of my antivirus software was ad ware so, like a fool I selected it for deletion before checking it. The antivirus went down like a stone. Antispy isn’t the only one that gives rise to false positives, but antivirus will also give false positives. Anyone ought to know about false positives, but I will give you my definition. A false positive is when any anti software is ran and the same anti software alerts of a virus, spyware, or adware although the anti software is in error.

Never choose to delete any file that is a false positive. “A question,” A lady stood up and asked, “what class would you class **Commodo internet security**? Is it a firewall or is it an antivirus?” The Practical Paranoid said, “well ma-am it is both, but we are jumping ahead a bit. Let’s take that topic up next. Let’s clear the air on all these programs so, we will not become confused.” A man asked, “are you using notes. I am curious.” The Practical Paranoid replied, “when I give a speech I never use notes. This is out of my memory. Let’s take up a very short topic and it will take only five minutes. Most websites have a topic called SECURITY TOOLS. This can mean anything like specialized antivirus programs,

encryption programs, and any other program that could not be classified by the traditional topics. **Threatfire** is a specialized software that can scan for rootkits. Just remember that a rootkit is spyware, but the people running the sites will put it under the above. **System Protect** which keeps a hacker or other person from altering any files is put under this heading. **My Lockbox** which is clearly an encryption program is also put under this heading."

A child stood up and asked, "why be careful with this stuff?" The practical paranoid said, "Well, one day I had a lot of music that I was going through it. A spyware thingy had did a scan and it gave a false positive. Well before checking what the processes I just had them removed. Well, my media players, readers, encryption, and internet when down. Every program on my system was a bunch of worthless junk. It had taken me an entire day just to repair it. Next we will discuss a piece of software called a firewall. Besides an antivirus this is what keeps hackers out of your system, but one last note. Look at the bottom of the page. Any questions? Next we will discuss the specialized antispy programs. Many times I will be repeating myself, but the information given is what I feel to be important."

ANTIMALWARE

This type of software is similar to antispyware. Using an on demand antimalware along with a system protector can keep this type of software off your system.

Norman Antimalware-This one is an excellent one to keep trojans from invading your system. I do a scan about once a month with this one.

A gentleman stood up and asked, "are there any more antimalware programs?" The practical paranoid said, "yes, but one must pay for them. Keep an eye on the sites listed because I am giving a few guidelines on securing your system."

The Practical Paranoid took a drink of water and cleared his throat then said, ""since we had spent a lot of time of antispyware and miscellaneous topics we will take a break. Stretch you legs, take a smoke, or get a snack. When we return we will cover creating a three to four tiered system."

He walked away from the podium and down into the audience and a person in computer security stopped him. He said, "this is commonsense stuff. Any reasonable person with a brain should know this stuff." The Practical Paranoid said, ""Well, you wait and we will get into stuff that will interest you. My background was that of Journalist, Corporate Spy, and electronic intelligence. I think you would be interested in the encryption." The guy nodded and let him leave.

Another woman confronted him, “what would be the best programs that are available?” The Practical Paranoid replied, “We will cover that later. I need some sugar and quickly. I do not want to pass out on the stage.” He then exited the stage and came back with a can of soda and sat down on the stage’s edge.

ANTIVIRUS

The Practical Paranoid once again took his place behind the podium and began, ““A piece of advice with regard to using antivirus software. I’ve created a computer system that possesses a primary and a secondary antivirus system. The secondary antivirus would be one that is an on-demand antivirus program. A person should set aside one day a week in which to scan their system. Here is a list of program combinations I had used to keep my system virus free. Some critics of the secondary antivirus would say that adding another antivirus would be overkill. Well, I would rather be safe than sorry. In my experience, I had my system crashed so many times I became very paranoid. I am the original Practical Paranoid. Let‘s now look on page 2 and 3 at the suites.”

Suite 1

AVG-Grisoft.com makes this antivirus. It is very good, but it can slow down an older
system.
Bitdefender 8 free-This one is an on-demand antivirus scanner.
Spyware terminator integrated with clam antivirus
360 antimalware integrated with advanced systemcare

Suite 2

AVG
Clam AV integrated with Spyware Terminator.
360 Antimalware integrated with advanced systemcare
System Protect

Suite 3

Avast
Clam AV integrated with spyware terminator
System Protect

Suite 4

Avast
Bitdefender free
Norman Antimalware

Suite 5

Antivir
Bitdefender free
Norman antimalware

Suite 6

Comodo Internet Security
AVG
Norman Antimalware

FILE ENCRYPTION

The practical paranoid said, “now we come to the fun stuff like keeping the cops out of your hair. The first layer of encryption ought to be a file encryptor. I use these for encryption layering a technique I discovered when I played with codes as a child. I could layer a substitution cypher to a point that it would take years to discover the message. Now, what ones of these are the best. There is a list of them in the booklet.”

Marx Bitware-This one in my opinion is the best, but it takes a while to encrypt files.

Zero Footprint Crypt-This one is like marx bitware. If you are in a hurry then forget it.

File waster-This one is very good, but not a very high level program. It is like the ones above.

Encrypt files-This one is very good.

File encryption-This one is also very good.

Androsa File Protector-This one is also good.

Crypt4Free-This one is good for low level encryption. Use the Blowfish 448 algorithm because it hasn’t been broken.

ENCRYPTED DRIVES

The practical paranoid said, “once you had encrypted the files then what? I put them into an encrypted drive. The list is given below the file encryption utilities.”

freeOTFE-This one is the one that contains the backdoor if you use the Microsoft CryptoAPI. Use mouse movement to create the drive. This thing can create a huge drive and I use a drive within a drive scheme.

Secret Drive-This one you can create a 4 GB drive. I would use the Blowfish algorithm because it hasn’t been cracked.

Discryptor-This one makes very tiny drives which are about 1 GB in size. I like the traveling drive which I will explain in a moment.

Truecrypt-This one can make drives of any size.

Comodo Disk Encryption-This one is the weakest of the encryption programs and I would not use it for high level encryption.

ENCRYPTED ZIP FILES

The practical paranoid said, “When I create a traveling drive I will zip the whole business into a encrypted zip file then I use a file protector. The encryption is only as good as its password.

BC-Archiver-I use this one for low level encryption.

FINAL TOUCHES TO OUR SYSTEM

"Now, we come to the final part of securing your system," replied the Practical Paranoid, "Turn to the last pages in the booklet. This is the proper use of drive scrubbers and drive scrubbers in general. We've covered trash removers and their dangers. This is how to keep stuff put on your system by hackers off your system.

I know some police types that will try to get your computer for nothing and plant evidence on it so they can get it. I‘ve had this done when I was a journalist and I had to flee into the forest. A rebel commander found me. I explained that the cops had seized my computer and all my belongings including a passport. He helped me get to the border and cross into another country."

A man stood up and shouted, "I am a policeman and we never did that." The Practical Paranoid let out a sound that sounded like a pig squeal and a series of oinks. The Practical Paranoid said, "If the shoe fits wear it. I have people I know that had charges trumped up by the likes of you. I know of people that had their cars seized by your type. I know of several that had their houses taken and their name ruined. Don't tell me any different. I know about police states and we are living in one. I was in a country that was ruled by the Military and they would kill anyone that would not agree with them in a heartbeat. News if you would call it that was censored by the government. Instead of capturing someone alive they murder them in bed and given the blessings of the leader. The sheeple would cheer and pat them on the back ATTA BOY JOB WELL DONE. They are given metals of valor for murder, pillage, plunder, and theft." The policeman sat down and remained quiet. The Practical Paranoid continued, "First, and most important. Set a restore point on your computer. I have my druthers and I use the drive wiper on C-cleaner set on high level, but it does not scrub your system well. Then I make an encrypted box to put all of my undeleted files into. Then this box would be erased.

COOKIE AND TRASH CLEANERS

C-cleaner-I use this one extensively. It does a good job, but the drive wiper leaves a lot to be desired.

Advanced Systemcare-This one is a good tune up suite. I use this one extensively.

Glary System Utilities-I use this one as well. It cleans the trash off left by other cleaners.

Which one of these are best. Well using all three of them would be sufficient to remove all the trash. The Big named utility suite took up 150MB of drive space. This one takes up 70MB of drive space. The Big Named utility suite did not do a good job either. In fact, it crashed my system shortly after installing it on a trial basis.

FORENSIC DRIVE SCRUBBERS

The practical paranoid said, “one last piece of information. I found one of the encrypted drive programs to have a backdoor on it. A backdoor is an entrance to

an encrypted drive without needing a password. That doesn't surprise me in these Police States of Amerika.

Freeraser-This one is good and I use it to destroy the encrypted drive full of garbage.

Eraser-This one gets excellent marks, but first before running it set a restore point.

Ultrawipe-Don't even use this one because it is not very good.

File shredder-This one is also good.

Next you will need a file recovery piece of software to check how good your scrubber had worked. I only do a deep cleaning about once every 3 to 4 months otherwise I just do a scrubbing of the freespace.

Recuva-This one is one of the best. I just put the stuff in an encrypted drive then I burn it with one of the programs above.

Pandora-This is an ad supported piece of software. I would not use it because it is adware.

Glary Utilities-This one possesses an excellent file recovery program. I've used it to find trash on my system.

Minitool Power Data Recovery-I've used this one to get back some files I had deleted. It seems to be a good one.

Tomorrow we will cover Encryption layering and how to secure information on your computer. Good night my friends and good luck.